precision
CYBERTECHNOLOGIES & DIGITAL SOLUTIONS LTD

CYBER DIGITAL WORLD

NEWSLETTER

Volume: 21 MAY 2023

Today we will be discussing cybersecurity as it relates to national security, why it has become increasingly important and what can be done to improve on it.

Dr. Ronald Walcott
Managing Director

Cybersecurity has become an integral part of our everyday lives. Almost every human on the face of the earth has some sensitive data and information about them that is valuable and is worth protecting. Whether it be medical records, financial records, criminal records, etc., it is all sensitive information that is to be highly guarded. With regards to national security, all this information getting into the wrong hands can pose a threat to a country's national security.

WHY CYBER SECURITY IS BECOMING INCREASINGLY IMPORTANT FOR NATIONAL SECURITY?

What is national security? National security refers to a government's ability to protect its citizens economy, and other institutions. This also means protecting the safety and overall well-being of all citizens within the country. In the 21st century national security includes non-military protection. All sectors, such as economic security, political security, energy security, homeland security, cybersecurity, human security, and environmental security need protection in the cyber/digital realm and encompasses national security.

In recent times, it is possible for hackers to attack from anywhere in the world, once they have a computer and an internet connection. Some countries engage in digital warfare by government organizations attacking different sectors in other country's government to either disrupt or steal/gain intel on sensitive information. And on the receiving end, the governments being targeted must be able to defend against these attacks and recover if they were hit. Countries must not only be able to defend against attacks from other governments, but also different hacker groups and individual hackers who are also very

In this Issue:

skilled and dangerous in the digital space. Hackers are able to leverage their different skills and also utilize AI (Artificial Intelligence) to help them break through defenses.

Here are a few of the reasons why cybersecurity is important for national security:

- **Protects against monetary losses** – one of the main motivations of a hacker, is monetary gain. Hackers steal or lock/block access to sensitive information and resources from the owners. They do so through malware such as ransomware, and viruses that infect your system. These external and untrusted software then either steals your information or locks your device or access to certain information & functionality and prompts you to pay a ransom in order to regain access to your device and resources. It takes a lot of money at times to recover resources or if the ransom is paid, you are not guaranteed to even regain access to what was taken, destroyed or restricted. An example of the monetary damage that hackers can cause to a country can be seen when we look at the incident that occurred on 31st May 2022 in Costa Rica. This attack costed the Costa Rican government millions of dollars in revenue, even though they refused to pay the ransom.
- **Loss of resources and functionality** – When hackers attack, a lot of the time resources are held hostage through DOS/DDOS (denial of service) attacks and malware (ransomware). For many companies and even sectors in the government, this can be extremely detrimental to them and their customers/clients. The organization loses money as more and more time passes while they do not have access to their resources to operate as normal or to an acceptable level. Again, we will look at the example of Costa Rica, where the Ministry of Public Works and Transport had 12 of their servers encrypted and their computer systems were knocked offline. This meant that services were briefly disrupted and services that were able to be done virtually had to revert to in-person until further notice.

We can see the disruptive power that hackers have on a national scale when cybersecurity is not optimally implemented or properly enforced. One of the world's leading governments, the American government, released the National Cyber Strategy in 2017. It was stated that "Advancing cybersecurity is a core priority". History clearly demonstrates that no single entity can meet and deal with this challenge alone. It is the responsibility of both public and private sectors to protect themselves and the interests of the public's national security. October was declared the International Cybersecurity Awareness month, 17 years ago, to build the attention to the importance to this area.

Frequently Asked Questions:

WHAT CAN THE GENERAL PUBLIC DO TO UPKEEP NATIONAL SECURITY WITH REGARDS TO CYBERSECURITY?

Everyone has a role to play in defending their national security. Someone can aid with this by taking little steps such as ensuring their personal information is secure and protected, and by also bringing awareness to others and educating them on the dangers that they face in this digital age.

WHO AND WHAT INDUSTRIES/SECTORS ARE MOST AT RISK OF BEING TARGETED BY HACKERS?

Hackers do not discriminate when it comes to their targets. They will target each and every vulnerable individual, company, sector, government and private organization. There everyone is equally at risk of being targeted by hackers. It simply comes down to who is the most vulnerable and who it would be more beneficial to attack.

HOW FREQUENTLY DO ATTACKS THREATEN NATIONAL SECURITY?

Every attack threatens national security regardless of how minor it may be. However, the severity of the attack, damage caused and financial impact of an attack can rapidly make an attack be a serious threat to national security. For example, if a hacker gets access to banking information or if a hacker hacks into a government sector like health care.

Upcoming Events

AI POWERED SASE IS HERE AND NOW
June 13, 2023
New York

AI POWERED SASE IS HERE AND NOW
June 15, 2023
Chicago

TIC (TRADE AND INVESTMENT CONVENTION)
July 20, 2023
Trinidad

Headline News

Dental Health Insurer Hack Affects Nearly 9 Million.

An insurance provider that services many state Medicaid agencies and children's health insurance programs told regulators that hackers compromised the personal and protected health information of nearly 9 million patients in an incident discovered in March. Fort Lauderdale, Florida-based MCNA insurance Company, in a data breach notification letter filed with the Maine state attorney general's office, said it detected unauthorized access to certain MCNA systems on March 6 and discovered that certain systems within the network were infected with malicious code.

The company also listed over 100 affected organizations impacted by the breach that includes the Arkansas Department of Human Services, the City of New York Management Benefit Fund, Florida Healthy Kids Corporation, the Idaho Department of Health and Welfare, the Iowa Department of Human Services, Louisiana Department of Health, Nebraska Department of Health and Human Services.

MCNA is a provider of dental and orthodontic care to members of certain state Medicaid agencies and the Children's Health Insurance Program, for which they provide dental benefits and services.

"Through its investigation, MCNA determined that an unauthorized third party was able to access certain systems and remove copies of some personal information between February 26, 2023, and March 7, 2023," the firm said in a sample breach notification letter.

MCNA's investigation found that the attackers were successful and that affected patient personal information may include full name, date of birth, address, telephone, email, social security number, and driver's license number or government-issued ID number.

The health data includes insurance information such as the name of plan/insurer/government payor, member/Medicaid/Medicare ID number, plan and/or group number and information regarding dental/orthodontic care. This information covered parents, guardians and guarantors, who paid the bill.

The attackers could also access data about patient visits, dentist names, doctor names, past care, X-rays/photos, medicines and treatment.

The extent to which data was compromised "was not the same for everyone," the firm said.

As of Friday, the MCNA Insurance incident did not yet appear on the U.S. Department of Health and Human Services website listing health data breaches affecting 500 or more individuals.